Principles of Cryptography Problem Sheet 1

Dr. Kurunandan Jain[1]†,

[1]Department of Mathematics, Amrita Vishwa, Amrita Campus, Kollam-690525, Kerala, India

(Received xx; revised xx; accepted xx)

1) Prove or disprove each statement

a) $6 \mid 42$

b) $64 \mid 50$

c) $16 \mid 0$

d) $0 \mid 15$

2) Compute the following results without a calculator

a) $15 \times 29 \bmod 13$

b) $2 \times 29 \bmod 13$

c) $2 \times 3 \bmod 13$

d) $-4 \times 3 \bmod 13$

3) What are the equivalence classes for $\bmod 7$.

4) We consider the ring $\mathbb{Z}_4$. Construst a table which describes the addition of all elements in the ring with each other:

a) Construct the multiplication table for $\mathbb{Z}_4$.

b) Construct the addition and multiplication tables for $\mathbb{Z}_5$.

c) Construct the addition and multiplication tables for $\mathbb{Z}_6$.

d) There are elements in $\mathbb{Z}_4$ and $\mathbb{Z}_6$ without a multiplicative inverse. Which elements are these? Why does a multiplicative inverse exist for all nonzero elements in $\mathbb{Z}_5$?

4) Compute x as far as possible without a calculator. Where appropriate, make sure a smart decomposition of the exponent as shown in class:

a) $x \equiv 3^2 \bmod 13$

b) $x \equiv 7^2 \bmod 13$

c) $x \equiv 3^{10} \bmod 13$

d) $x \equiv 7^{100} \bmod 13$

e) $7^x \equiv 11 \bmod 13$

5) This problem deals with the affine cipher with the key parameters $a = 7$ and $b = 22$

a) Decrpyt the text: falszztysyjzyjkywjrztyjztyynaryjkyswarztyegyyj

6) The ciphertext below was encrypted using a substitution cipher. Decrypt the ciphertext without knowledge of the key

lrvmnir bpr sumvbwvr jx bpr lmiwv yjeryrkbi jx qmbm wi bpr xjvni mkd ymibrut jx irhx wi bpr riirkvr jx ymbinlmtmipw utn qmumbr dj w ipmhh but bj rhnvwdmbr bpr yjeryrkbi jx bpr qmbm mvvjudwko bj yt wkbrusurbmbwjk lmird jk xjubt trmui jx ibndt

wb wi kjb mk rmit bmiq bj rashmwk rmvp yjeryrkb mkd wbi iwokwxwvmkvr mkd ijyr ynib urymwk nkrashmwkrd bj ower m vjyshrbr rashmkmbwjk jkr cjnhd pmer bj lr fnmhwxwrd mkd wkiswurd bj invp mk rabrkb bpmb pr vjnhd urmvp bpr ibmbr jx rkhwopbrkrd ywkd vmsmlhr jx urvjokwgwko ijnkdhrii ijnkd mkd ipmsrhrii ipmsr w dj kjb drry ytirhx bpr xwkmh mnbpjuwbt lnb yt rasruwrkvr cwbp qmbm pmi hrxb kj djnlb bpmb bpr xjhhjcwko wi bpr sujsru msshwvmbwjk mkd wkbrusurbmbwjk w jxxru yt bprjuwri wk bpr pjsr bpmb bpr riirkvr jx jqwkmcmk qmumbr cwhh urymwk wkbmvb

† Email address for correspondence: kurunandanj@am.amrita.edu

a) Compute the relative frequency of all the letters A· Z in the ciphertext.

b) Decrypt the ciphertext with the help of the relative letter frequency of the English language.

7) Using the keyword: Puck and Vigenre Cipher, what is the corresponding ciphertext for the plaintext: What fools these mortals be

8) Using the keyword: Thanos and Beaufort Cipher, what is the corresponding ciphertext for the plaintext: Avengers Assemble

9) Now, we want to extend the affine cipher, such that we can encrypt and decrypt messages written with the full German alphabet. The German alphabet consits of the English one together with the three umlauts, Ä, Ö, Ü and the even stranger ”double s” character ß.

a) What are the encryption and decryption equations for this cipher?

b) How large is the key space of the affine cipher for this alphabet?

c) The following ciphertext was encrypted using the key $a = 17, b = 1$. What is the corresponding plaintext?

Ä U ßw ß

Hint: Ä→ 26, Ö→ 27, Ü→ 28 and ß→ 29